NEC

文書管理番号：SND-SEC-MI-21003-1.7

Deep Security Agent 20.0
アップグレード手順書
(Windows)

2024 年 10 月 21 日

【第 1.7 版】

日本電気株式会社

更新履歴

項番	版数	更新日	更新内容	更新箇所	更新区分	備考
1	1.0	2021/09/27	—	—	新規	
2	1.1	2022/03/23	特定の更新プログラムの適用が必要な OS があることを追記	1.2 動作環境	更新	
3	1.2	2023/01/17	対応 OS を更新 Windows の最小バージョン要件について追記	1.2 動作環境	更新	
4	1.3	2023/10/10	サポート期間が終了した OS の Deep Security Agent 20.0 でのサポート内容が変更されます	1.2 動作環境	更新	
5	1.3	2023/10/10	サポート対象の Web ブラウザを記載	2.3 管理サーバログイン	更新	
6	1.4	2024/01/23	"https://success.trendmicro.com/jp/" で始まる URL を最新のものに変更	1.2 動作環境	更新	
7	1.4	2024/01/23	以下の内容を追記 ※Deep Security Agent 20.0 未満はサポート対象外です。	1.2 動作環境	更新	
8	1.5	2024/06/25	限定サポート対象 OS の制限事項について記載	1.2 動作環境	更新	
9	1.5	2024/06/25	記載内容を修正	1.1 本資料について	更新	
10	1.6	2024/08/14	製品 Q&A の URL を更新	1.2 動作環境	更新	
11	1.6	2024/08/14	記載内容を修正	2, 2.1, 2.2, 2.3, 2.4, 3	更新	
12	1.7	2024/10/21	記載内容を修正	1.2 動作環境	更新	

目 次

1 はじめに

1.1 本資料に関して

本資料は、Windows 環境において「Deep Security Agent 20.0」をご利用のお客様が、バージョンアップを行う方法を記載しています。

1.2 動作環境

（1）Deep Security Agent 20.0 は、以下の動作環境を満たしている必要があります

メモリ	最小 RAM 2GB ※5GB 以上を推奨
ハードディスク	1GB 以上を推奨
OS	Windows 7 (32- and 64-bit) Windows 7 Embedded (32-bit) Windows 8 (32- and 64-bit) Windows 8.1 (32- and 64-bit) Windows 8.1 Embedded (32-bit) Windows 10 (32- and 64-bit) Windows 10 IoT Enterprise 2019 LTSC (32- and 64-bit) Windows 10 IoT Enterprise 2021 LTSC (64-bit) Windows 10 Enterprise multi-session (64-bit) Windows 11 (64-bit) Windows Server 2008 (32- and 64-bit) Windows Server 2008 R2 (64-bit) Windows Server 2012 (64-bit) Windows Server 2012 R2 (64-bit) Windows Server 2016 (LTSC, version 1607) (64-bit) Windows Server Core (SAC, version 1709) (64-bit) Windows Server 2019 (LTSC, version 1809) (64-bit) Windows Server 2022 (LTSC, version 21H2) (64-bit)

※ **下記リンク先に記載の各 OS に対応したマイクロソフト社の更新プログラムを適用してください**
Windows の最小バージョン要件に記載のセキュリティパッチが適用されていない場合、2023 年 2 月中旬以降にリリースされる ACS で署名された Deep Security Agent を適用した後、**正常に動作しません**。

2023 年 2 月以降に公開されるトレンドマイクロのサーバおよびエンドポイント製品、および関連モジュールに関する Windows の最小バージョン要件について
[参照先]：https://success.trendmicro.com/ja-JP/solution/KA-0013632

リリース日は以下の URL から確認ください
[参照先]：https://help.deepsecurity.trendmicro.com/ja-jp/software.html
※ 「長期サポート（LTS)」タブには 2 世代分しか表示されないので「長期サポート（LTS)」タブに記載がない場合は「以前のバージョン」タブをご確認ください

※ 2024 年 1 月 1 日より OS ベンダーが定めるサポート終了後、原則 1 年間の通常サポートを提供した上で、「限定サポート」の提供へと移行します。詳細は以下の製品 Q&A をご参照ください。
[参照先]：https://success.trendmicro.com/ja-JP/solution/KA-0014849

※ 限定サポート対象 OS の制限事項
限定サポート対象となっているレガシーOS は、次回の改訂した新しい DSA 20.0.x から
システム要件外になります。

例)
2024 年 1 月以降にリリースされた DSA 20.0.1-xxx は、2023/12/31 時点での
限定サポート OS 上では、ご利用いただけません。(システム要件外となります。)
※誤ってアップグレードおよび新規インストールを行った場合は、不可である旨のエラー/警告が出力されます。

現在の限定サポート対象 OS は以下の製品 Q&A をご参照ください。
[参照先]：https://success.trendmicro.com/ja-JP/solution/KA-0015528

※ エディションが指定されていない Windows 製品は、エディションに関係なく動作を保証いたします。

※ システム要件に記載されていない Service Pack 等でも、要件に記載されているものより新しいバージョンはサポート対象となります。

※ Deep Security Agent 20.0 未満はサポート対象外です。
Deep Security Agent 20.0 は、リリース日から 5 年後の 12 月 31 日でサポート終了します。
[参照先]：https://success.trendmicro.com/ja-JP/solution/KA-0009810#ds20

※ 下記の OS については、各 OS に対応したマイクロソフト社の更新プログラムを適用してください。

- Windows 7 SP1　KB3033929 / KB4490628
- Windows Server 2008 SP2　KB2763674 / KB4474419
- Windows Server 2008 R2 SP1　KB3033929 / KB4490628

参考情報
コードサイニング証明書(コード署名証明書)における対応方針について
https://success.trendmicro.com/ja-JP/solution/KA-0006042

（2）本製品の利用には下記の要件を満たす必要があります。

- インターネット接続が可能
- TCP443 で通信が可能
- プロキシ経由する場合は、プロキシの認証無し、もしくは Basic 認証で通信が可能（Digest 認証と NTLM 認証は未サポート。）
- 保護対象サーバが以下の URL にアクセスできる必要があります。
- 保護対象サーバから対象 URL への通信経路に FW やロードバランサなどの通信機器が存在する場合は、SSL を含む送信、受信が共に可能な設定となっていることをご確認ください。
- 「仮想パッチ&アンチウイルスライセンス」のライセンスをご利用で、機械学習型検索をご利用の場合は以下 URL の「Smart Protection Network -Global Census サービス」「Smart Protection Network - Good File Reputation サービス」「Smart Protection Network -機械学習型検索」の項目に記載の URL にアクセスできる必要があります。（https://help.deepsecurity.trendmicro.com/20_0/on-premise/ja-jp/communication-ports-urls-ip.html）

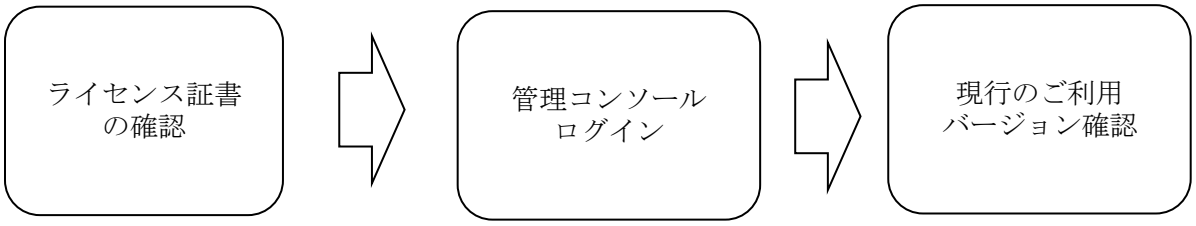
URL	用途	補足
serversecurity-nec.jp:443	管理コンソール URL	保護対象サーバ上で管理コンソールにアクセスしない場合は不要です。
hb.serversecurity-nec.jp:443	管理サーバとの疎通確認、イベントログの送信等	
reray.serversecurity-nec.jp:443	セキュリティアップデート ソフトウェアアップデート	
iaus.trendmicro.com:443	セキュリティアップデート	Trend Micro 社 Active Update サーバ。 アクセス可能にすることで可用性が向上します。
iaus.activeupdate.trendmicro.com 443		
ipv6-aus.trendmicro.com:443		
ipv6-iaus.activeupdate.trendmicro.com:443		

2 事前準備

2.1 事前準備

【注意事項】
・事前準備作業は、保護対象サーバ以外のお客様のクライアント PC や端末機でも実施可能です。

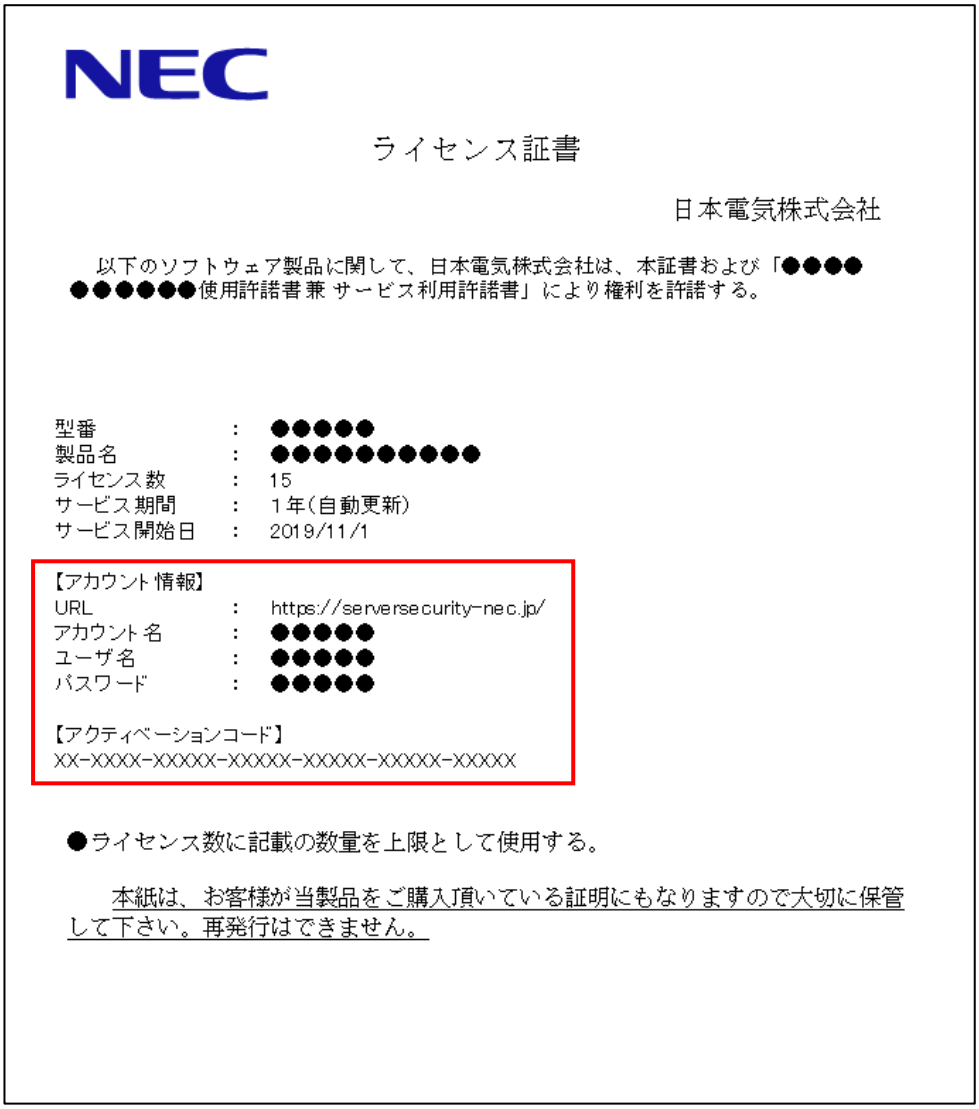
Agent 導入前に管理コンソール上で、Agent インストールの事前準備を行います。



2.2 ライセンス証書の確認

【注意事項】
・この情報は、管理コンソールログイン等に使用します。
・外部に公開しない様、慎重にお取り扱いください。

別途送付したライセンス証書より、アカウント情報（赤枠部分）を確認してください。



NEC

ライセンス証書

日本電気株式会社

以下のソフトウェア製品に関して、日本電気株式会社は、本証書および「●●●●●●●●●●●使用許諾書 兼 サービス利用許諾書」により権利を許諾する。

型番　：　●●●●●
製品名　：　●●●●●●●●●●
ライセンス数　：　15
サービス期間　：　1年(自動更新)
サービス開始日　：　2019/11/1

【アカウント情報】
URL　：　https://serversecurity-nec.jp/
アカウント名　：　●●●●●
ユーザ名　：　●●●●●
パスワード　：　●●●●●

【アクティベーションコード】
XX-XXXX-XXXXX-XXXXX-XXXXX-XXXXX-XXXXX-XXXXX

●ライセンス数に記載の数量を上限として使用する。

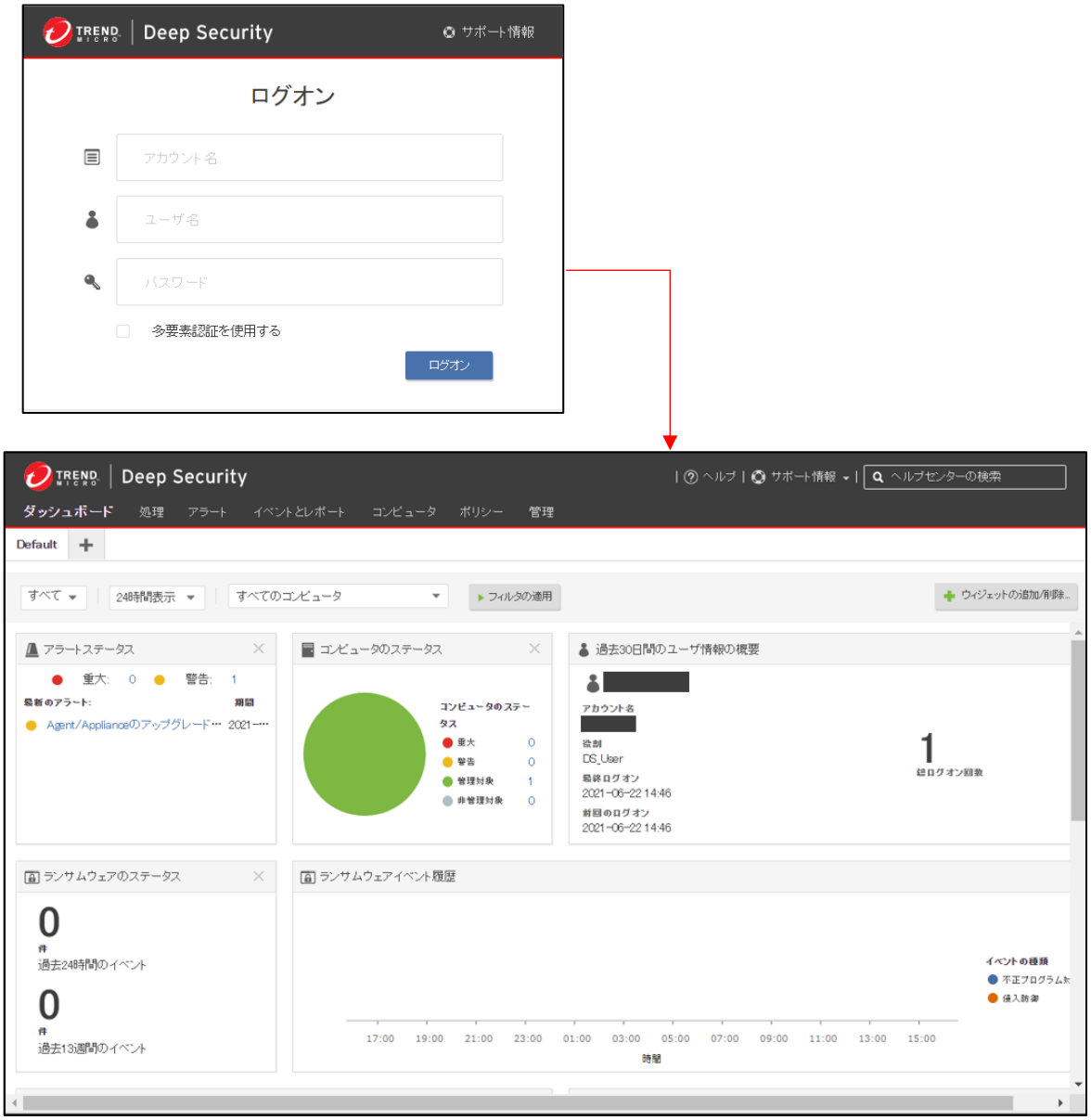
本紙は、お客様が当製品をご購入頂いている証明にもなりますので大切に保管して下さい。再発行はできません。

2.3 管理コンソールログイン

【注意事項】
管理コンソールは以下の Web ブラウザで動作を保証します。
- Mozilla Firefox (Cookie を有効にする)
- Microsoft Edge (Cookie を有効にする)
- Google Chrome (Cookie を有効にする)
- Safari (Cookie を有効にする)

(1) ライセンス証書の[アカウント情報] > [URL] に記載してある URL にアクセス

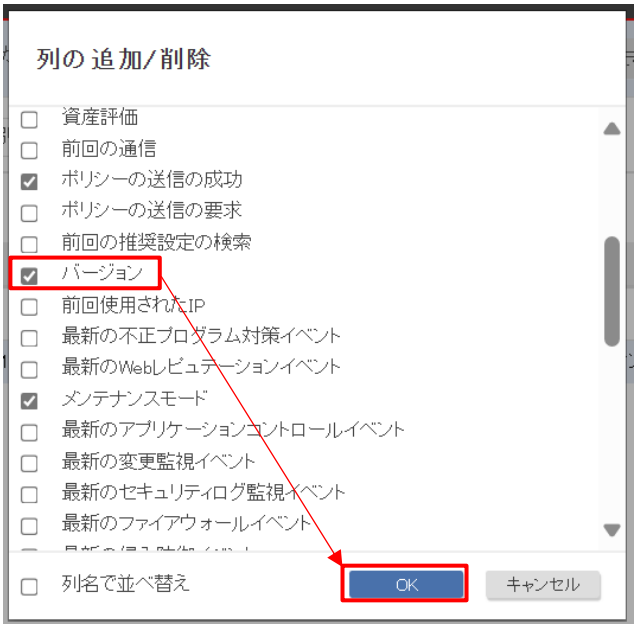
(2) ライセンス証書の[アカウント情報] > [アカウント名/ユーザ名/パスワード]を入力してログイン



2.4 現行のご利用バージョンの確認

(1) [コンピュータ] > [列]を選択

(2) [バージョン」にチェックボックスを入れ、「OK」ボタンをクリック



(3) [バージョン]列から確認

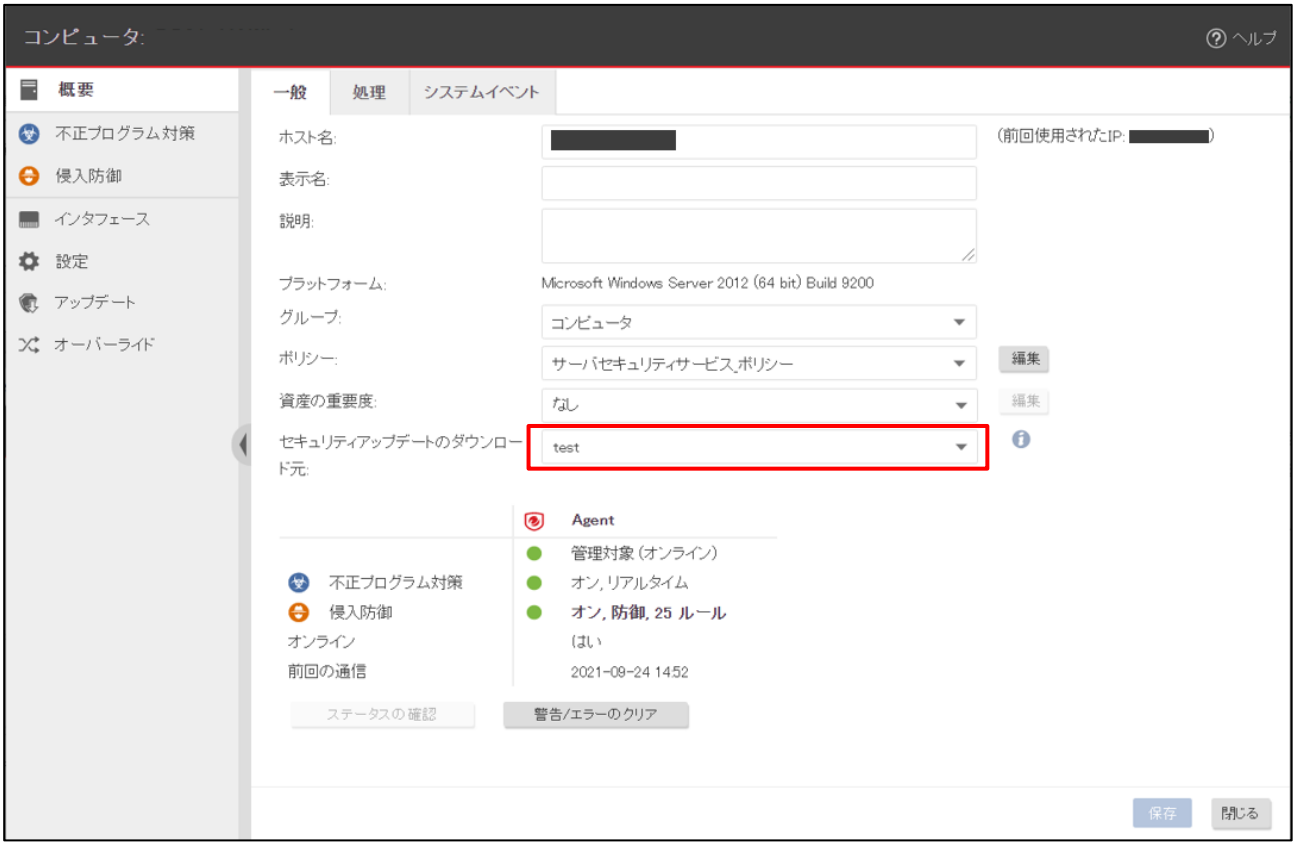
2.5 セキュリティアップデートのダウンロード元の変更

【注意事項】
※プロキシを経由しない環境の場合、本手順は不要です

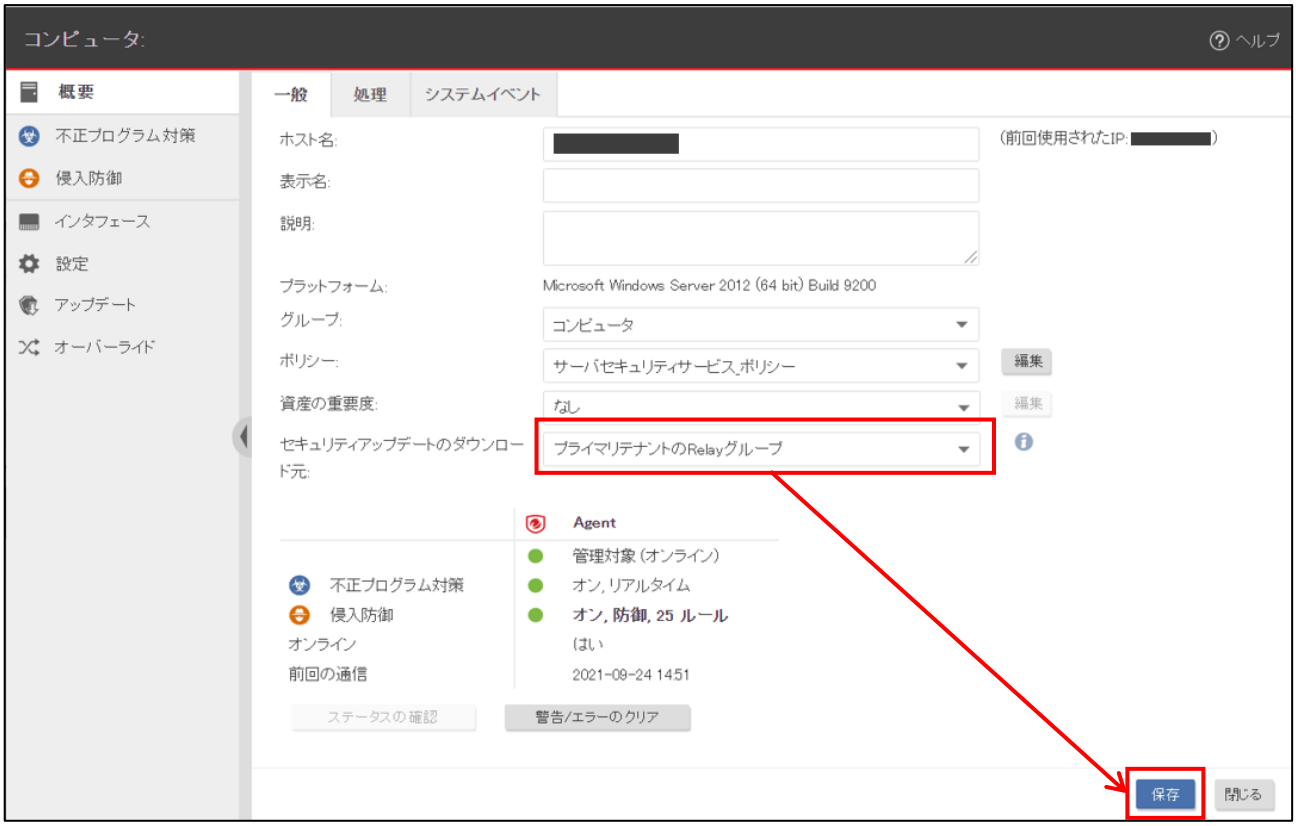
(1) 管理コンソールにログイン

(2) [コンピュータ]タブを選択

(3) 対象のコンピュータの詳細画面を表示し、[概要]の[一般]タブで、[セキュリティアップデートのダウンロード元:]に、”プライマリテナントの Relay グループ”以外が設定されていることを確認する。
※”プライマリテナントの Relay グループ”が設定されている場合は以降の手順は不要です。



(4) [セキュリティアップデートのダウンロード元:]のプルダウンリストから”プライマリテナントのRelay グループ”を選択し、[保存]をクリックする。



2.6 Relay への接続に使用するプロキシの設定

【注意事項】
※既に Relay のプロキシ設定をしている場合やプロキシを使用しない場合、本手順は不要です。

（1）Agent をインストールしたホストでコマンドプロンプトを管理者権限で開く

（2）「cd [DeepSecurityAgent をインストールしたフォルダ]」を入力し[Enter]を押下

【参考】
デフォルト設定の場合は、下記のフォルダ移動コマンドを入力ください。
cd "C:¥Program Files¥Trend Micro¥Deep Security Agent"

（3）以下のコマンドを実行し、Relay へ接続するためのプロキシを設定する。
dsa_control -y relay_proxy://*プロキシサーバの URL:ポート*//

「HTTP Status: 200 - OK」と表示されれば完了。

プロキシで認証（Basic 認証のみ対応）を行う場合、
「dsa_control -y relay_proxy://*プロキシサーバの URL:ポート*//」行の次行に、

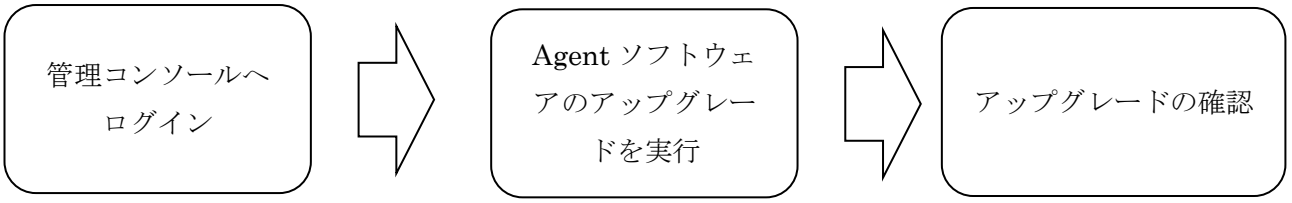
「dsa_control -w *ユーザ名:パスワード*」

と入力してください。

例）「ユーザ名：root、パスワード：Password」の場合、以下のように入力
dsa_control -w root:Password

3 アップグレードする手順

管理コンソールにログインし、Agent ソフトウェアのアップグレードを実行します。

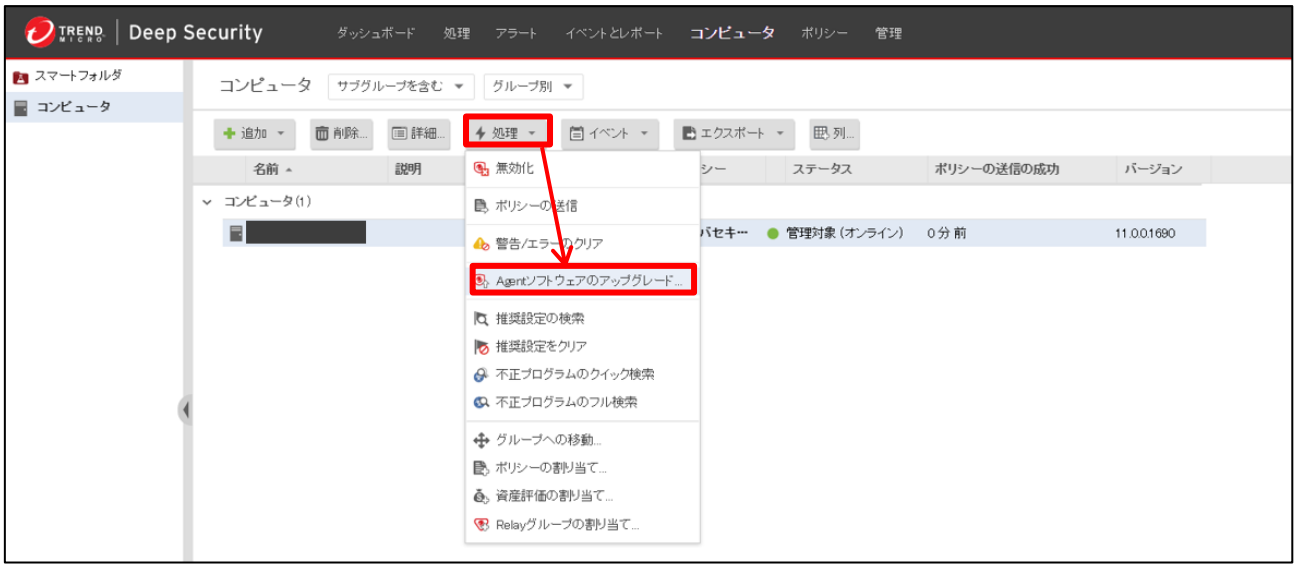


3.1 Agent ソフトウェアのアップグレードを実行する

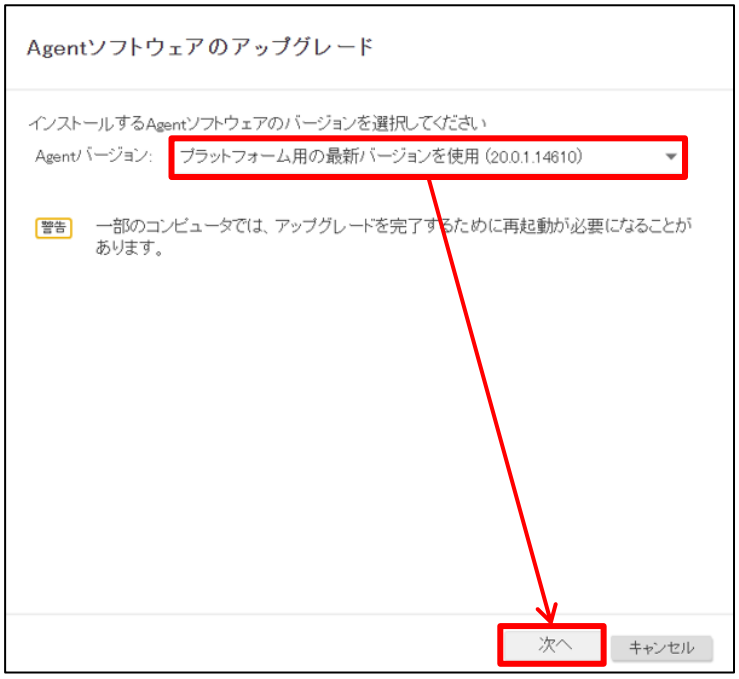
（1）管理コンソールへログイン

（2）[コンピュータ]タブを選択

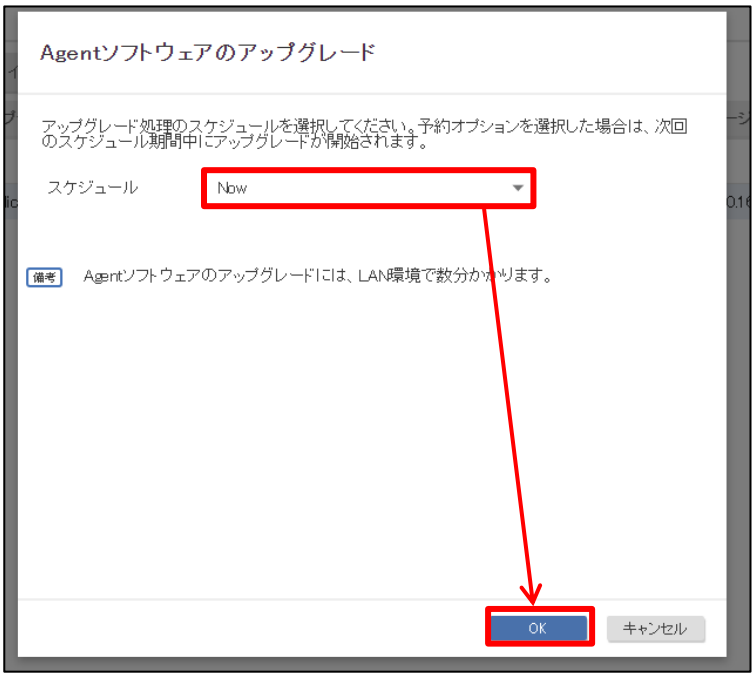
（3）[処理] > [Agent ソフトウェアのアップグレード]をクリック



（4）[20.0.1-]に続く数値が一番大きなバージョンを選択して、[次へ]をクリック



（5）スケジュールは[Now]を選択し、[OK]をクリック



（6）アップグレードの完了を待つ。最新のバージョンになっていることを確認する。

（参考）モジュールのインストール失敗のエラーが発生した場合

アップグレード処理時、一時的に「ソフトウェアアップデート：〇〇モジュールのインストール失敗」のエラーが発生することが確認されています。

当該エラーはアップグレード処理における一時的なものですので、警告/エラーのクリアを押下し、しばらく後に状況をご確認ください。